U.S. Customs and Border Protection

INTEGRATED FIXED TOWERS (IFT) SYSTEM OPERATIONAL REQUIREMENTS DOCUMENT (ORD)

DOCUMENT NO: OTIA05-IFT-00-000001

Version: A, September 27, 2011

DEVELOPED BY:
OFFICE OF TECHNOLOGY INNOVATION & ACQUISITION (OTIA)
OPERATIONAL INTEGRATION AND ANALYSIS DIRECTORATE (OIAD)

Operational Requirements Document (ORD)

for

CBP Integrated Fixed Towers (IFT)

Version A of September 27, 2011

Endorsed by: (b) (6), (b) (7)(C)
Joint Requirements Council

6-mar-12
Date

Approved by: (b) (6), (b) (7)(C)
Under Secretary for Management
Acquisition Decision Authority

3/15/12
Date

Stakeholder Signature Page

Submitted by: (b) (6), (b) (7)(C) 9/28/11
Date
Executive Director (Acting), OIAD

Endorsed by: (b) (6), (b) (7)(C) 9/28/11
Date
Program Manager, Integrated Fixed Towers

Endorsed by: (b) (6), (b) (7)(C) 6 DEC 2011
Date
Chief, United States Border Patrol

Endorsed by: (b) (6), (b) (7)(C) 19 Dec 2011
Date
Component Acquisition Executive

Endorsed by: (b) (6), (b) (7)(C) 6-Mar-2012
Date
Department of Homeland Security

Endorsed by: See title page dated 15 March 2012
Date
Acquisition Decision Authority
Department of Homeland Security

Approved by: Not Required per D-102
Date
(b) (6), (b) (7)(C)
Commissioner, Customs and Border Protection

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The Department of Homeland Security (DHS) is charged with managing, securing, and controlling the nation's borders with a priority mission focus of preventing terrorists and terrorist weapons from entering the United States (U.S.). The U.S. Customs and Border Protection (CBP) represents the front line in the defense of our nation's borders. In support of the CBP 2009-2014 Strategic Plan, the United States Border Patrol (USBP) is tasked with the responsibility of securing the nation's borders against the illegal entry of people and goods between Ports of Entry (POE). While the ultimate goal is deterrence, USBP uses a mix of infrastructure, technology, and personnel to establish and maintain effective control of the land borders. These resources are used to execute the mission essential tasks of predicting illicit activity, detecting and tracking border crossings, identifying and classifying the detections, and responding to and resolving suspect border crossings.

The October 2006 Secure Border Initiative (SBI) Mission Need Statement (MNS) identifies a number of capability gaps in USBP's ability to execute its mission. To address those gaps, the Arizona Border Surveillance Technology Plan identifies a number of technologies to be deployed in accordance with local operational needs and constraints. One of those technology approaches is Integrated Fixed Towers (IFT) systems. These systems provide long range persistent surveillance to enable USBP personnel to detect, track, identify and classify illegal entries through a series of integrated sensors and a common operating picture (COP). This document defines the operational requirements for IFT and provides the following information:

- Section 1: Restates the applicable mission needs and gaps, provides background regarding the Arizona Border Surveillance Technology Plan and discusses initial and final operational capabilities.

- Section 2: Discusses the CBP mission functions and how IFT supports those functions, provides a high level summary of the concept of operations, defines the high level operational requirements for IFT and defines the critical operational issues (COI) that IFT should address.

- Section 3: Defines the effectiveness requirements for IFT systems.

- Section 4: Defines the suitability requirements for IFT systems.

- Section 5: Summarizes the IFT Key Performance Parameters (KPP).

To execute the Arizona Border Surveillance Technology Plan and provide persistent surveillance capability at designated geographical locations by the end of Fiscal Year 2013, CBP is seeking non-developmental items (NDI), Government Off-the-Shelf (GOTS), or Commercial Off-the-Shelf (COTS). Because NDI/GOTS/COTS may not meet all operational requirements, Appendix 2 prioritizes the requirements to facilitate cost-effectiveness and schedule tradeoffs. Deviations to operational requirements should be coordinated with USBP as described in Appendix 2.

REVISION HISTORY

REV	DATE	DESCRIPTION
A	09-27-2011	Initial Release

1 INTRODUCTION

1.1 PURPOSE

DHS is charged with managing, securing, and controlling the nation's borders with a priority mission focus of preventing terrorists and terrorist weapons from entering the U.S. CBP represents the front line in the defense of our nation's borders. CBP's activities are organized into three mission sets: **(1) Securing America's Borders; (2) Securing and Expediting the Movement of People and the Flow of Goods, and (3) Sustaining Investment in its People and Capabilities**.[1] USBP has the responsibility of securing the nation's borders against the illegal entry of people and goods between POE. To accomplish this, USBP uses a mix of infrastructure, technology, and personnel to manage the land borders. These three resources are used to execute the mission functions of predicting illicit activity, detecting and tracking illegal border crossings, identifying and classifying the incursions, and responding to and resolving those incursions.

To efficiently and effectively manage the Nation's borders, USBP requires persistent surveillance and Command, Control, Communication, Coordination and Intelligence (C4I) capabilities. Both enhance overall situational awareness and, coupled with the right mix of manpower and tactical infrastructure, enhance operational effectiveness to counter a dynamic and evolving border threat. However, critical gaps in these capabilities were articulated in the October 2006 SBI Mission Needs Statement (MNS):

1. Detection and Tracking
2. Identification and Classification
3. Situational Awareness and a Common Operating Picture (COP)

The SBInet Program was intended to provide solutions to address these capability gaps. Through the SBInet Block 1 deployment and the addition of (b) (7)(E) USBP has experienced operational gains and increased situational awareness where these systems have been deployed. However, as of January 2011, SBInet Block 1 covers (b) (7)(E) border (b) (7)(E) (b) (7)(E) (b) (7)(E)

The Arizona Border Surveillance Technology Plan is a major change in direction compared to SBInet. Where SBInet represented an attempt to develop a system that would meet ambitious requirements, including a requirement for comprehensive networking and integration among sensor and communications, the new plan is much more modest. It consists of tailored deployment of stand-alone, non-developmental (and ideally commercial) sensor systems. There is no initial effort intended to integrate or network any of the individual systems. Over time, as personnel become more familiar with the operations and potential of these systems, their experience may provide a basis for future enhancements and increased performance. However,

[1] CBP's Missions, Goals, and Priorities, FY2011-2013

for now, the intent is to avoid "over-shooting" mission needs at all costs, and delivering low-risk systems that can give immediate support to the overall border security mission.

Within the new technology plan, one of the stand-alone systems will be the IFTs. Since the IFTs will be non-developmental, GOTS, or COTS, CBP will select from among commercial offerings which represent the best balance among performance and cost trade-offs. This Operational Requirements Document (ORD), therefore, is a framework for that trade-off but it does not represent (nor is it intended to represent) a firm set of requirements that must be met by the eventual IFT system. In fact, this ORD will be supplemented to record and reflect the final acquisition decision that results from the trade-offs. Put another way, the IFT will be a "capability-based" procurement. This ORD reflects the capabilities that are of general interest for IFT.

The purpose of this document is to define the operational requirements, KPPs and COIs that will be a point of departure for IFT systems. These requirements were developed through an Integrated Product Team, authorized under CBP's Office of Technology Innovation and Acquisition. The team was comprised of USBP agents, technology subject matter experts, systems engineers, and acquisition professionals. The requirements development process included market research and analysis of the original SBInet requirement to assess, among many other factors, performance, testability, and affordability. The operational requirements also consider results from the SBInet operational test.

1.2 BACKGROUND

In 2005, DHS established the SBI, a comprehensive, multi-year plan to help secure America's borders. The SBI Program Office deployed SBInet, an IFT-like system (b) (7)(E) that (b) (7)(E) SBInet provides coverage (b) (7)(E) of the southwest border within Tucson Sector. Operational requirements for SBInet are defined in the SBInet Operational Requirements Document, Version 1.0, March 6, 2007. That document remains applicable to the SBInet systems; however, CBP has since refined operational requirements for future IFT deployments. CBP has also reassessed the overall surveillance technology approach using a DHS-directed analysis of alternatives (AoA). This AoA measured the effectiveness of various technological initiatives while considering key assumptions in funding levels, program timelines, and potential changes in the broader immigration environment. The initial phase of the AoA validated the basic mission need to "maintain awareness of border activity through persistent surveillance." The AoA evaluated four system alternatives to meet this need along the southwest border:

- Agent centric systems
- Aviation centric systems
- Mobile, decentralized systems
- Fixed systems with centralized/integrated control centers (i.e. IFT)

The most effective and efficient implementation of these technology alternatives depends on the specifics of a given area, such as, terrain, geography, population, concept of operations and

enforcement tactics. IFT solutions, for example, can provide (b) (7)(E) in remote terrain, (b) (7)(E). This layered technology approach, one that positions the most appropriate technology alternatives according to local operational considerations, provides the most cost-effective approach to managing the border. The results of the AoA are summarized in the Arizona Border Surveillance Technology Plan.

1.3 INITIAL OPERATIONAL CAPABILITY AND TIMELINE

CBP is seeking commercial or non-developmental items that provide (b) (7)(E) (b) (7)(E) to enable the detection, tracking, identification, and classification of illegal entries in rural and remote areas. Because it is unlikely that NDI or COTS/GOTS can meet all requirements in Sections 3 and 4, USBP has prioritized the requirements in Appendix 2 to facilitate cost-effectiveness and schedule tradeoffs. The objective timeline for the initial operational capability (IOC) is the second quarter of Fiscal Year 2013, and the threshold is the fourth quarter of Fiscal Year 2013.

IOC is defined as the following geographical segments (pending final USBP analysis):

- (b) (7)(E) Station Command and Control Center
- (b) (7)(E) IFT units located across the (b) (7)(E) Station AoR

1.4 FULL OPERATIONAL CAPABILITY AND TIMELINE

The operational requirements for Full Operational Capability (FOC) are the same as the IOC requirements. FOC timeline is estimated for completion in Fiscal Year 2015 and is defined as the following additional geographical segments (pending final USBP analysis):

- (b) (7)(E) Station Command and Control Center
- (b) (7)(E) IFT units located across the (b) (7)(E) Station AoR

- (b) (7)(E) Station Command and Control Centers
- (b) (7)(E) IFT units located across the (b) (7)(E) Station AoR

- (b) (7)(E) Station Command and Control Center
- (b) (7)(E) IFT units located across the (b) (7)(E) Station AoR

- (b) (7)(E) Station Command and Control Center
- (b) (7)(E) IFT units located across the (b) (7)(E) Station AoR

While FOC is currently limited to the Arizona border, the operational requirements also consider the environments along the remainder of the southern border, and the northern border as an objective, given the likelihood that IFT capabilities will be needed beyond Arizona.

2 MISSION REQUIREMENTS

Objective 1.1 in CBP's 2009-2014 Strategic Plan states that CBP must: "*Establish and maintain effective control of air, land, and maritime borders through the use of the appropriate mix of infrastructure, technology and personnel. A segment of the border between ports of entry is considered under effective control when CBP can simultaneously and consistently achieve the following: (1)* ***detect*** *illegal entries into the United States; (2)* ***identify*** *and* ***classify*** *these entries to determine the level of threat involved; (3) efficiently and effectively* ***respond*** *to these entries; and (4) bring each event to a satisfactory law enforcement* ***resolution.***"

CBP's key mission elements (i.e. mission essential tasks) are defined below in Table 1; those mission elements directly supported through IFT capability are predict, detect, track, identify/classify, and respond.

Table 1 CBP Mission Elements[2]

Mission Element	Definition
Predict	To anticipate illegal traffic actions prior to illegal activity
Deter	To dissuade illegal cross border activity into and out of the United States by creating and conveying a certainty of detection and apprehension
Detect	To discover possible illegal traffic
Track	To follow the progress/movements of possible illegal traffic
Identify	To determine what the detected entity is (human, animal, conveyance, unknown)
Classify	To determine the level of threat or intent of the detected entity
Respond	To employ the appropriate level of law enforcement resources to successfully address illegal traffic
Resolve	To take final CBP action, whether criminally, administratively, or other, against apprehended illegal traffic. [This includes capture data, process information, etc. This may also include the release of legitimate traffic with no law enforcement action.]

To successfully execute these mission elements, USBP requires a number of operational capabilities that include:

[2] Definitions from Secure Border Initiative Design Reference Mission Version 1.0, Dated 14 May 2010

- Persistent Surveillance Capability: the ability to continuously detect, track, identify and classify border incursions 24 hours a day, 7 days a week (24/7) in targeted areas under all weather, terrain, vegetation and lighting conditions
- Command, Control, Communication, Coordination and Intelligence (C4I) Capability: the ability to collect and analyze information, exchange information and intelligence, allocate and control resources according to operational needs, and make informed operational command decisions in support of the mission
- Sustainment and Support Capability: the ability to maintain and sustain the surveillance systems in accordance with mission needs and operational requirements

Persistent surveillance is a critical capability needed to manage border areas exploited by the threat. (b) (7)(E) coupled with C4I capabilities, enables USBP to efficiently and effectively manage rural and remote areas of interest (AoI).[3] Historical data demonstrate how border threats adapt quickly to counter CBP operations. Accordingly, USBP leverages (b) (7)(E) capabilities to the greatest extent possible (b) (7)(E) Furthermore, dedicated field agents are required to operate these systems – (b) (7)(E) field agents to cover a twenty-four hour period. IFT system units (comprised of the individual (b) (7)(E) provide a (b) (7)(E) alternative with (b) (7)(E) of a surv ultiple IFT units are integrated into a COP at a command and control center, IFT systems enable USBP to monitor very large areas of coverage (AoC)[5] within an AoI with fewer agent and equipment resources. IFT systems contribute to situational awareness, agent safety and are a preferred solution in certain rural and remote areas that are difficult to access and/or where USBP has a need for longer term/permanent persistent surveillance because of a persistent threat. As one part of a multi-layered approach to border surveillance, IFT will contribute to both the persistent surveillance and C4I capabilities needed by USBP.

To reiterate – with respect to the IFT program, these requirements are a framework for evaluating and selecting among NDI, GOTS, or COTS systems. The actual procurement will be a capability-based one that reflects appropriate trade-offs among performance and cost. As indicated elsewhere in this document, all performance requirements are prioritized and may be waived to reflect the results of the capability-based procurement, consistent with the terms of this ORD.

[3] An AoI is defined as a targeted area within a USBP Station's AoR that requires surveillance due to the risk level associated with the border threat exploitation. Note – there may be more than one AoI within an AoR.

[4] The "surveillance area" is defined as the area within which a single IFT unit is capable of detecting, tracking, identifying and classifying illegal incursions.

[5] The AoC is defined as the resulting area, considering installation location of all IFT units, view shed and line of sight obstructions, etc., within which USBP can successfully conduct surveillance activities using the IFT system. When used in a broader context, AoC can also refer to the coverage provided by a combination of surveillance systems.

2.1 OPERATIONAL REQUIREMENTS

USBP requires the capability to continuously monitor a targeted AoI 24/7, to enable the detection, tracking, identification and classification of illegal traffic, as follows:

- (b) (7)(E)

While there are no specific operational requirements for persistent surveillance or C4I that trace to the deter mission element, historical data indicate that a high probability of apprehension resulting from the persistent surveillance of an AoI will ultimately result in deterrence of illegal incursions within that AoI.

The operational requirements articulated above are high level operational requirements descriptions. Specific IFT operational requirements that support these needs are specified in Sections 3 and 4, which further quantify the system features and attributes necessary to achieve these operational needs. Table 5 in Appendix 2 summarizes the operational requirements and provides traceability to the COIs, mission elements and capabilities. Table 5 also prioritizes the operational requirements to facilitate cost-effectiveness tradeoffs given resource constraints and the operational need to deploy this capability by the end of Fiscal Year 2013.

Because the operational needs, tactics and geographical constraints vary widely across the AoI where IFT systems will be used, several of the effectiveness requirements in Section 3 focus on the level of performance expected from a *single IFT unit*, rather than defining the overall "installed" AoC of a group of IFT units that will be a function of lay down, surrounding terrain, vegetation, foliage, etc.

[6] Near real-time is defined to be a (b) (7)(E) to facilitate effective employment of the system.

2.2 CRITICAL OPERATIONAL ISSUES

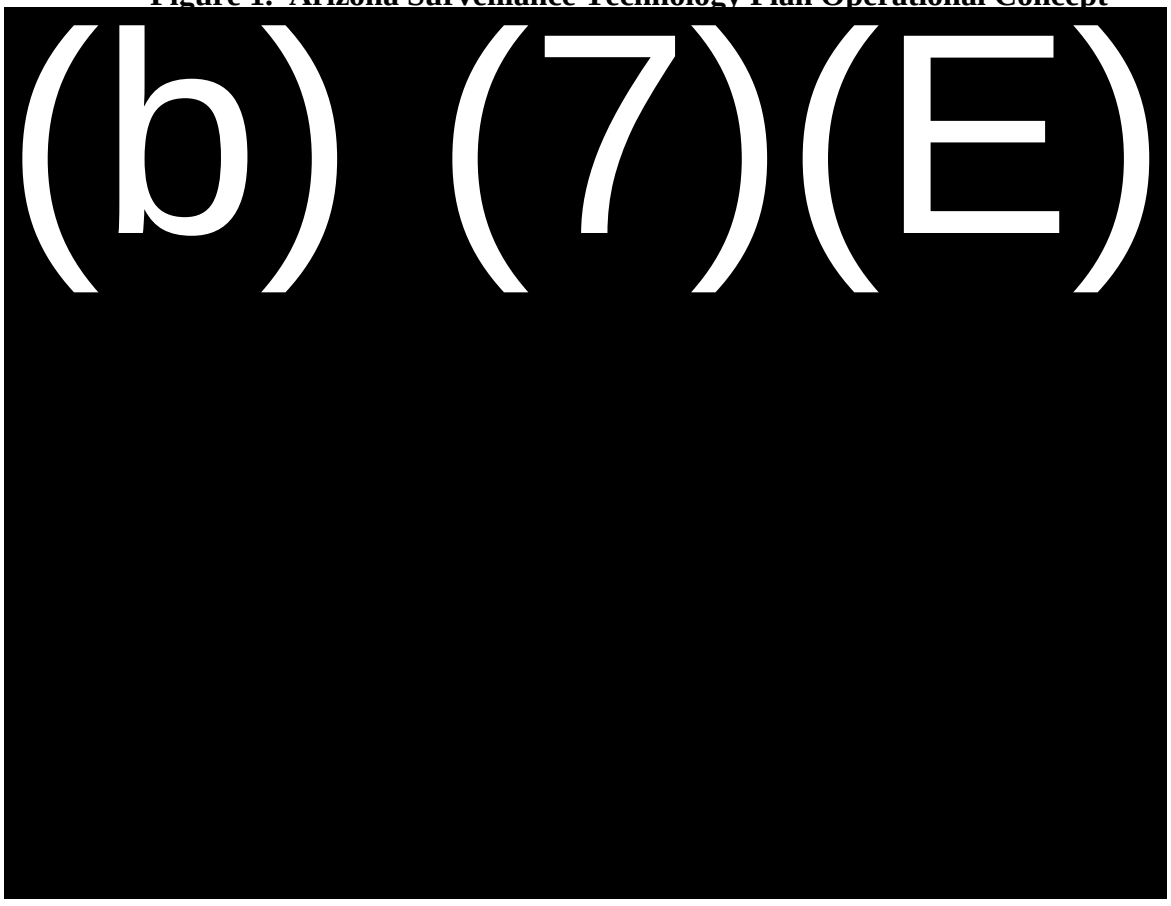
The effectiveness and suitability critical operational issues (COI) to be assessed during operational test are listed below. Any changes to these COIs as they are further developed and decomposed will be documented in the IFT Test and Evaluation Master Plan:

COI#1 – Does the IFT system provide persistent surveillance of IoIs within the Arizona Border AoCs?
COI#2 – Does the IFT system assist Border Patrol personnel with command and control decisions regarding the resolution of IoIs within the Arizona Border AoCs?
COI#3 – Does the IFT system operate satisfactorily in field environments along the Arizona Border?

2.3 CONCEPT OF OPERATION

Figure 1 illustrates notionally how USBP employs a layered, defense-in-depth surveillance approach to manage land borders between POE. This layered approach incorporates fixed surveillance capabilities (such as IFT, (b) (7)(E), and Unattended Ground Sensors (UGS)), and (b) (7)(E) as needed to effectively manage the border and reduce risk.

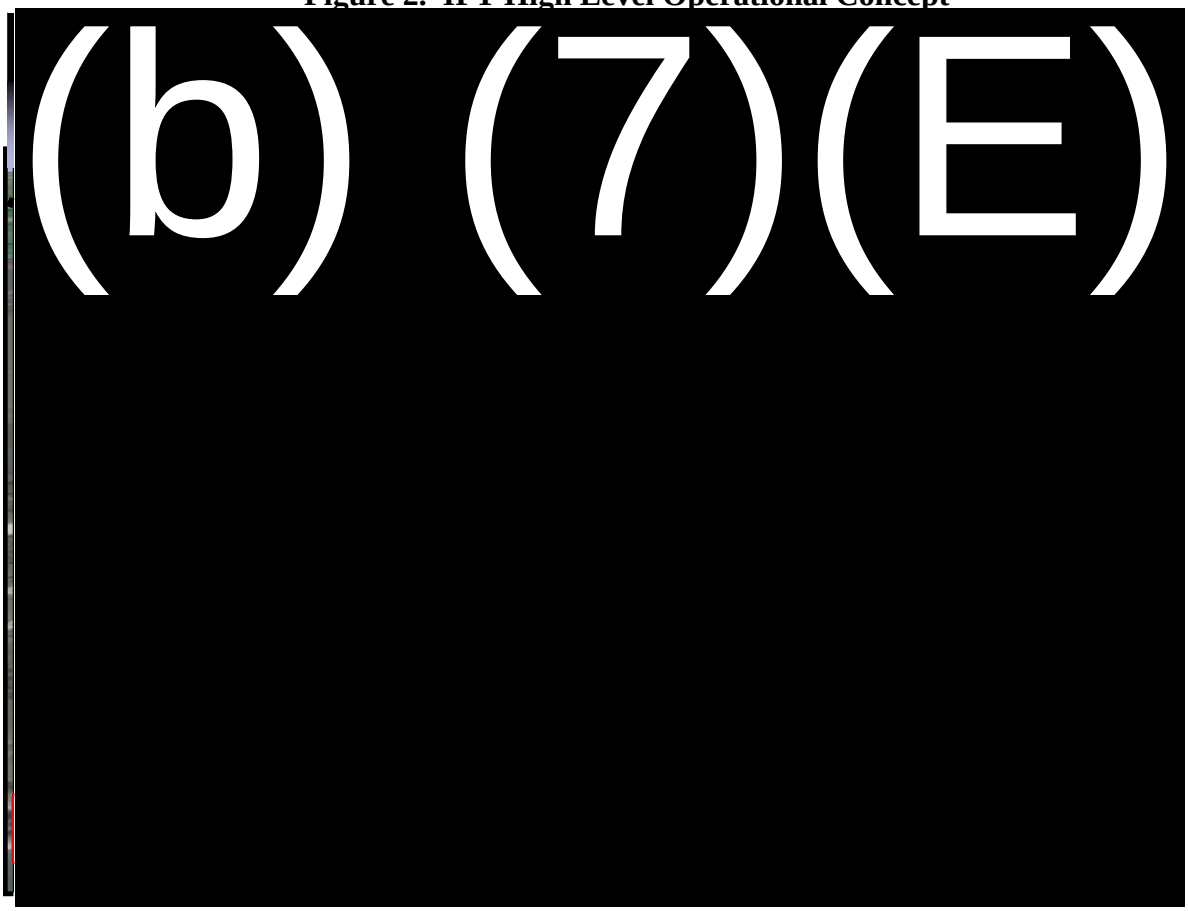
Figure 1. Arizona Surveillance Technology Plan Operational Concept



IFT systems will provide (b) (7)(E) persistent surveillance capability in those areas where the AoA determined that they are the most cost-effective surveillance solution considering local operational needs and constraints. An IFT system (displayed notionally in Figure 2) will consist of a (b) (7)(E) . Each IFT unit will consist of a (b) (7)(E) The systems will continuously detect and track IoIs across a targeted AoC, (b) (7)(E) The IFT high level operational concept is shown in Figure 2.

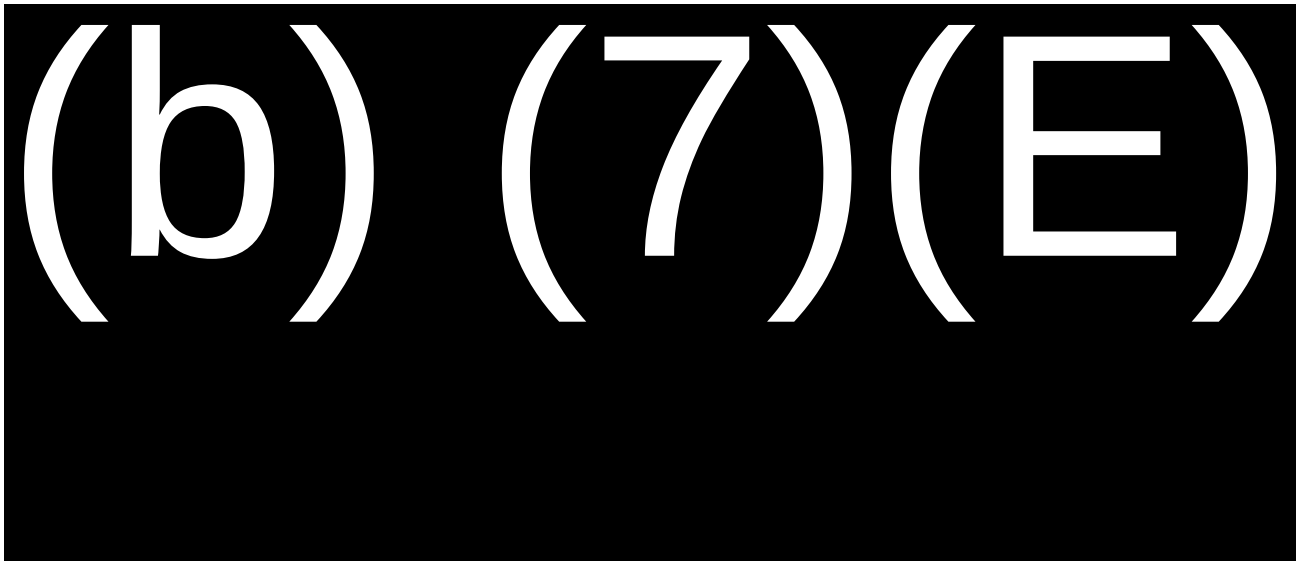
[7] Note: (b) (7)(E) .

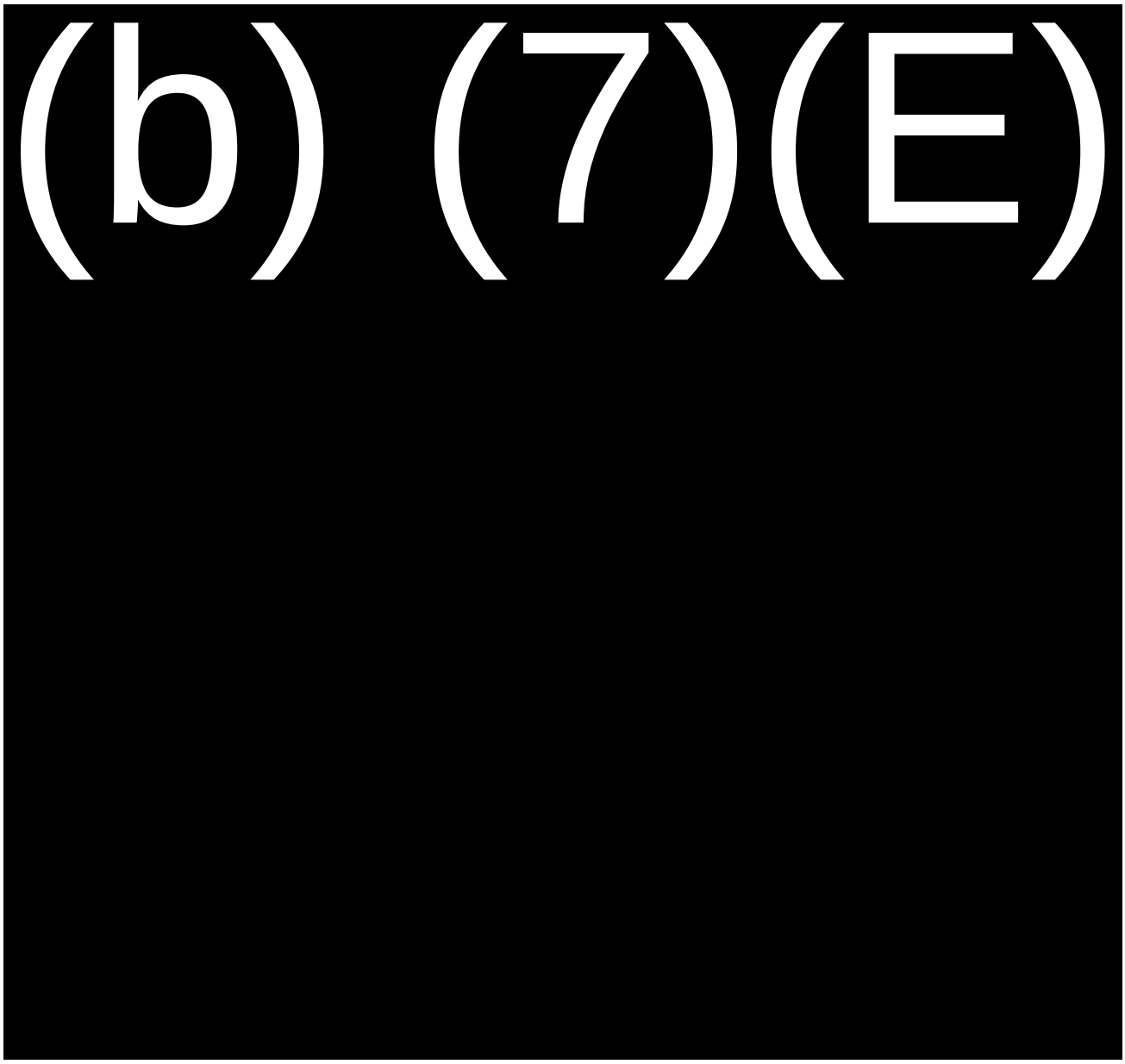
Figure 2. IFT High Level Operational Concept



The IFT system will accomplish the following tasks:

- Detect any IoI that enters the AoC
- Track all detected IoIs as they move within the AoC





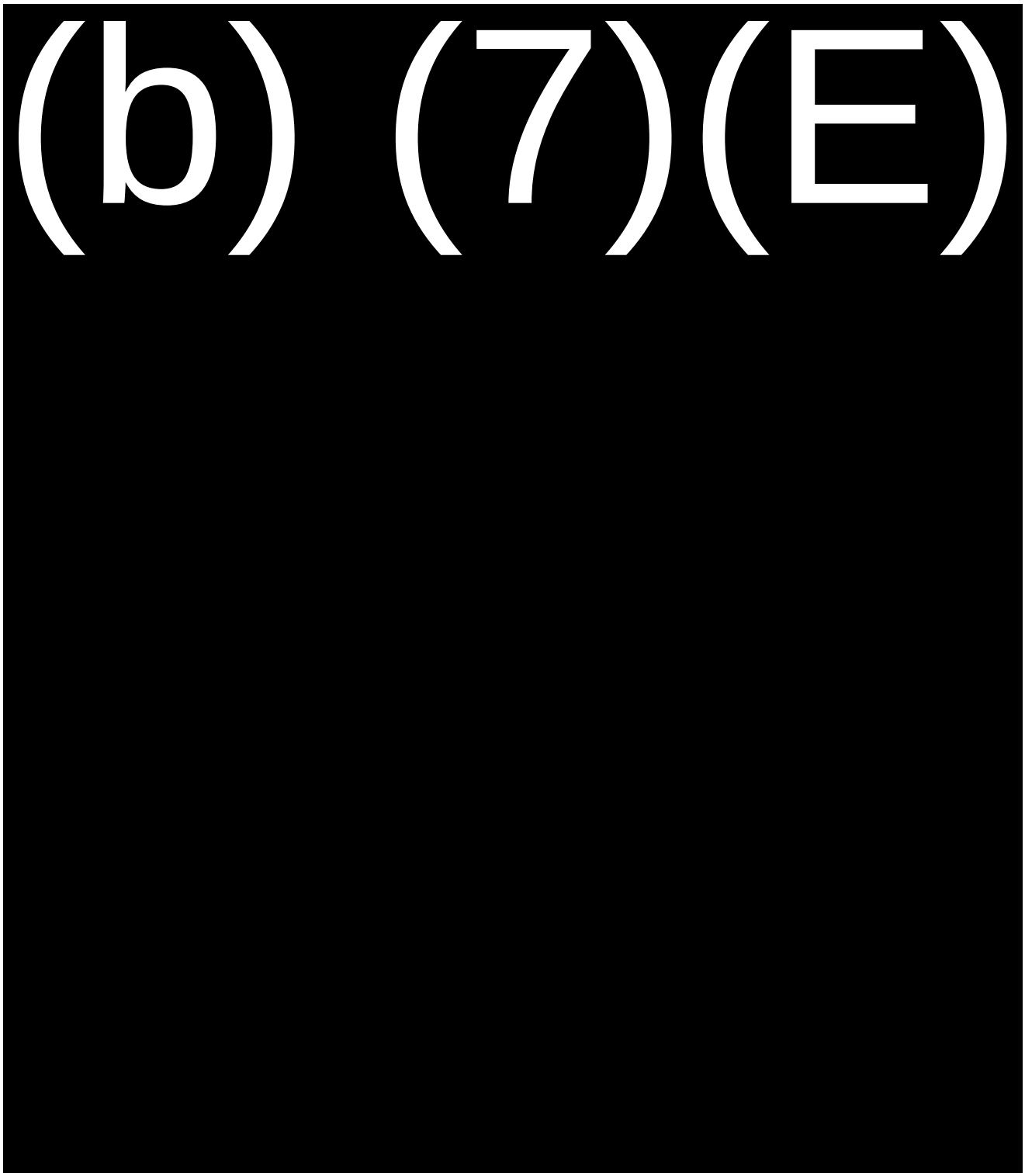
Note: operational test results on SBI*net* indicate that operator proficiency is maximized through the use of documented tactics, techniques and procedures (TTP), and through a dedicated pool of trained operators who can develop proficiencies operating the system.[8] Accordingly, each USBP station employing IFT may institute an IFT Team comprised of agents or sector enforcement specialists (or both) trained to operate the system who remain on the team for a specified period of time.

For additional information on the concept of operations for IFT and other surveillance systems, see the *Arizona Border Surveillance Technology Plan Concept of Operations Document*.

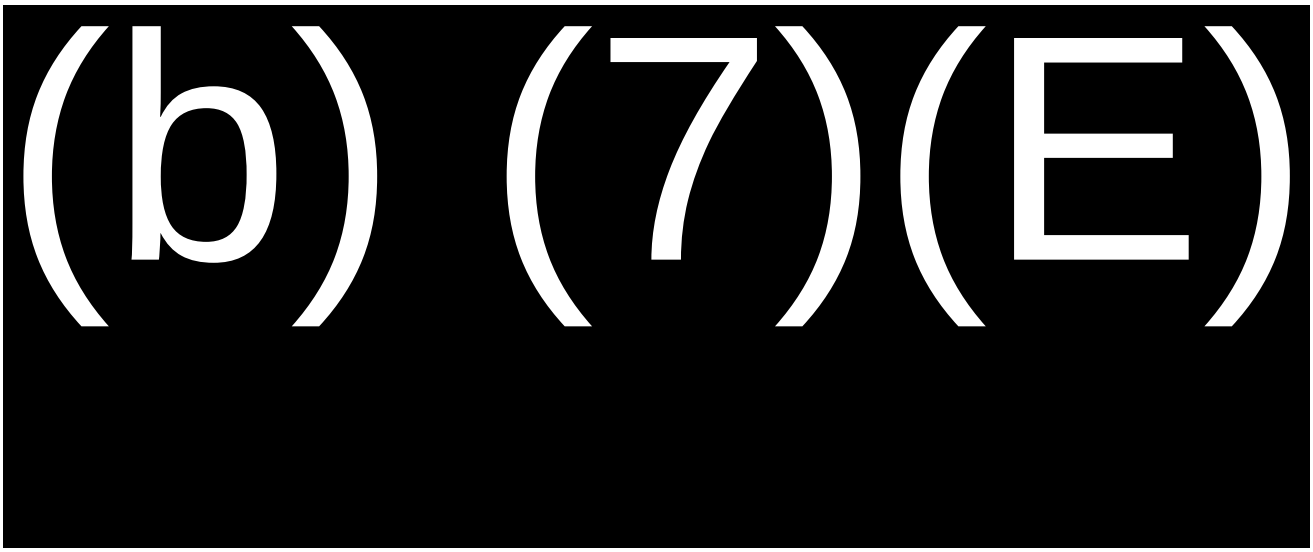
[8] Operational Test Agency Evaluation Report for the Secure Border Initiative Network (SBInet) Block 1.0, March 2011.

2.4 OPERATIONAL SCENARIOS

The following scenarios describe the activities agents will perform to execute their missions and how they will utilize the IFT capability.




(b) (7)(E)



2.5 CONCEPT OF SUPPORT

2.5.1 MAINTENANCE AND SUPPORT

The IFT system will perform mission-critical functions 24/7. As such, maintenance and sustainment support will also be required 24/7 to minimize system down time associated with scheduled and unscheduled maintenance.

The maintenance approach will employ two levels of maintenance: organizational and depot. The system will employ health status/monitoring capability in order to quickly identify and report mission critical failures to the operator and the maintainers. Mission critical failures include any condition that prevents the system from performing the mission elements it's designed to perform. Once a mission critical failure has been identified, the operator will contact a helpdesk for assistance with troubleshooting the problem. If the problem is not resolved, authorized technicians will perform site repairs on the assets. For safety reasons, (b) (7)(E) (b) (7)(E) depending on the site, (b) (7)(E) (b) (7)(E) (b) (7)(E)

Appropriate measures will be recorded and used to assess the following metrics: mean time between critical failures (MTBCF), mean time to repair (MTTR) the system and the failed part, mean logistics delay time (MLDT), mean down time (MDT)[9], operational availability (Ao), high mortality components, and other metrics useful for predicting/planning ongoing operations and maintenance.

The maintenance and logistics support approach should ensure the continued capability and availability of the surveillance systems at best cost through the annual Operational Analysis conducted to determine if the investment is meeting its performance goals. Each Operational Analysis should assess compliance with all KPPs.

[9] MDT is the sum of MTTR and MLDT.

2.5.2 TRAINING

A comprehensive training program will be developed to support both the operation and maintenance of IFT systems. Operator and Train the Trainer (T3) training will be implemented through CBP's Office of Training and Development, and maintainer training will be implemented through the Office of Information and Technology (OIT). The training will encompass the necessary classroom, on-the-job, and computer-based training in support of BP's mission and supportability requirements.

3 EFFECTIVENESS REQUIREMENTS

The following requirements describe the basic performance attributes required by IFT in support of Persistent Surveillance and C4I capabilities. Thresholds (T) and objectives (O) are defined where applicable, and KPPs are highlighted in bold. Requirements that do not specify a threshold or objective are, by default, threshold requirements. As noted previously, the operational needs, tactics and geographical constraints vary widely across the AoI where IFT systems will be used, so several of the effectiveness requirements focus on the level of performance expected within the surveillance area of a *single IFT unit*. To reiterate – with respect to the IFT program, these requirements are a framework for evaluating and selecting among NDI, GOTS, or COTS systems. The actual procurement will be a capability-based one that reflects appropriate trade-offs among performance and cost. As indicated elsewhere in this document, all performance requirements are prioritized and may be waived to reflect the results of the capability-based procurement, consistent with the terms of this ORD.

3.1 PERSISTENT SURVEILLANCE

The following requirements are applicable 24/7 to a surveillance area (b) (7)(E) (b) (7)(E) prescribed in Section 4.9, unless otherwise noted.

3.1.1 DETECT AND TRACK

IFT ORD 01 A single IFT unit shall provide a surveillance area (b) (7)(E)

Rationale: (b) (7)(E)

IFT ORD 02 A single IFT unit shall, (b) (7)(E)

Rationale: (b) (7)(E)

.

IFT ORD 03 **A single IFT unit shall** (b) (7)(E)

Rationale: (b) (7)(E)

IFT ORD 04 A single IFT unit shall (b) (7)(E)

Rationale: (b) (7)(E)

IFT ORD 05 The system shall (b) (7)(E)

Rationale: (b) (7)(E)

IFT ORD 06 The system shall (b) (7)(E)

Rationale: (b) (7)(E)

IFT ORD 07 A single IFT unit shall (b) (7)(E) .

Rationale: (b) (7)(E)

IFT ORD 08 A single IFT unit shall (b) (7)(E)

Rationale: (b) (7)(E)

IFT ORD 09 The system shall (b) (7)(E)

Rationale: (b) (7)(E)

3.1.2 IDENTIFY AND CLASSIFY

IFT ORD 10 The system shall provide (b) (7)(E)

Rationale: (b) (7)(E)

IFT ORD 11 The system shall provide (b) (7)(E)

[10] (b) (7)(E) . This is applicable to all IFT units within an IFT system.

Rationale: (b) (7)(E)

IFT ORD 12 The system shall provide (b) (7)(E)

Rationale: (b) (7)(E)

IFT ORD 71 The system shall provide (b) (7)(E)

Rationale (b) (7)(E)

.

3.2 COMMAND, CONTROL, COMMUNICATION AND INTELLIGENCE

3.2.1 SYSTEM REMOTE COMMAND AND CONTROL (C2)

IFT ORD 13 The system shall provide the operator (b) (7)(E)

Rationale: (b) (7)(E)

IFT ORD 14 The system shall (b) (7)(E)

Rationale: (b) (7)(E)

(b) (7)(E)

3.2.2 COMMUNICATION

IFT ORD 15 The system shall (b) (7)(E)

Rationale: (b) (7)(E)

3.2.3 OPERATOR INTERFACE AND TOOLS

IFT ORD 16 The system shall (b) (7)(E)

Rationale: (b) (7)(E)

IFT ORD 72 The system shall provide (b) (7)(E)

Rationale: (b) (7)(E)

IFT ORD 17 The system shall enable the operator to (b) (7)(E)

Rationale: (b) (7)(E)

IFT ORD 18 The system shall enable the operator to (b) (7)(E)

Rationale: (b) (7)(E)

IFT ORD 19 The system shall (b) (7)(E)

Rationale: (b) (7)(E)

IFT ORD 20 The system shall enable the operator (b) (7)(E)

Rationale: (b) (7)(E)

IFT ORD 21 The system shall enable the operator to (b) (7)(E).

Rationale: (b) (7)(E)

IFT ORD 22 The system shall (b) (7)(E)

Rationale: (b) (7)(E)

IFT ORD 23 The system shall (b) (7)(E)

Rationale: (b) (7)(E)

IFT ORD 24 The system shall enable the operator to (b) (7)(E)

Rationale: (b) (7)(E)

IFT ORD 25 The system shall provide the functionality and configurability to (b) (7)(E)

Rationale: (b) (7)(E)

IFT ORD 26 The system shall (b) (7)(E) .

Rationale: (b) (7)(E) .

IFT ORD 27 The system (b) (7)(E)

Rationale: (b) (7)(E)

IFT ORD 28 The system shall provide (b) (7)(E) .

Rationale: (b) (7)(E) .

IFT ORD 29 The system shall provide an operator (b) (7)(E)

Rationale: (b) (7)(E)

IFT ORD 30 The system shall enable USBP-authorized personnel (b) (7)(E)

Rationale: (b) (7)(E)

IFT ORD 31 The system shall enable the operator to (b) (7)(E)

Rationale: (b) (7)(E)

IFT ORD 32 The system shall enable the operator to (b) (7)(E) n.

Rationale: (b) (7)(E)

IFT ORD 33 The system shall geospatially display the international boundary line.

Rationale: The COP operator needs the ability to assess the location of IoIs in relation to the border for situational awareness.

3.2.4 RESPONSE SUPPORT

IFT ORD 34 The system shall provide the means for the operator (b) (7)(E)

Rationale: (b) (7)(E)

IFT ORD 35 The system shall (b) (7)(E)

Rationale: (b) (7)(E)

IFT ORD 36 The system shall (b) (7)(E) .

Rationale: (b) (7)(E)

3.2.5 PREDICT (INTELLIGENCE) AND REPORTING SUPPORT

IFT ORD 37 The system shall, without operator intervention (b) (7)(E)

(b) (7)(E)

Rationale: (b) (7)(E)

IFT ORD 38 The system shall enable the operator to (b) (7)(E)

Rationale: (b) (7)(E) .

IFT ORD 39 The system shall enable the operator to (b) (7)(E)

Rationale (b) (7)(E) .

IFT ORD 40 The system shall enable USBP-authorized personnel to (b) (7)(E)

Rationale: (b) (7)(E)

3.3 INTEROPERABILITY

IFT ORD 41 The system shall (b) (7)(E)

Rationale: (b) (7)(E)

IFT ORD 42 The system shall (b) (7)(E)

Rationale: (b) (7)(E)

IFT ORD 43 The system shal (b) (7)(E)

Rationale: (b) (7)(E)

.

IFT ORD 44 The system shall (b) (7)(E)

Rationale: (b) (7)(E)

.

IFT ORD 45 The system shall be capable of (b) (7)(E)

Rationale: (b) (7)(E)

IFT ORD 46 The system shall be capable of utilizing existing CBP communications infrastructure when such infrastructure is available.

Rationale: The ability to leverage existing capabilities reduces the logistics footprint and life cycle cost.

IFT ORD 47 The system shall be capable of (b) (7)(E)

Rationale: (b) (7)(E)

IFT ORD 48 The system shall (b) (7)(E)

Rationale: (b) (7)(E)

4 SUITABILITY REQUIREMENTS

The following requirements describe the basic attributes required in support of sustainment and support capabilities. To reiterate – with respect to the IFT program, these requirements are a framework for evaluating and selecting among NDI, GOTS, or COTS systems. The actual procurement will be a capability-based one that reflects appropriate trade-offs among performance and cost. As indicated elsewhere in this document, all performance requirements are prioritized and may be waived to reflect the results of the capability-based procurement, consistent with the terms of this ORD.

4.1 DESIGN

IFT ORD 49 The system shall not interfere with or degrade the operation of other CBP equipment.

Rationale: The system must be compatible with existing equipment.

IFT ORD 50 The system shall be approved for secure operations in accordance with applicable CBP and DHS security policies and procedures.

Rationale: As stated.

IFT ORD 51 The system shall (b) (7)(E)

Rationale (b) (7)(E)

IFT ORD 52 The system shall provide (b) (7)(E)

Rationale: (b) (7)(E) .

4.2 RELIABILITY

IFT ORD 53 Reserved.

IFT ORD 54 (b) (7)(E) .

Rationale: (b) (7)(E)

4.3 AVAILABILITY

IFT ORD 55 **The system operational availability (Ao) shall be equal to or greater than** (b) (7)(E) **where Ao is defined as mission capable time (sum of all mission critical subsystems and units) divided by total time (mission capable time plus down time). (KPP**)

Rationale: USBP must perform critical mission elements 24/7 without significant disruption or degraded capability. A system is considered operationally available when it can perform in accordance with the operational requirements. A system is not mission capable under any condition that precludes the detection, tracking, identification or classification of IoIs within an AoC (when the system would otherwise be capable of doing so).

4.4 MAINTAINABILITY

IFT ORD 56 The system MDT shall be less than or equal to (b) (7)(E)

Rationale: While USBP seeks to minimize system down time, a shorter MDT requirement could dictate (b) (7)(E)

IFT ORD 57 The system shall report mission critical failures to the operator (T) / and provide system health status when prompted by the operator (O).

Rationale: The system performs mission critical functions; as such, the operator must know when the system is unable to perform these functions so that appropriate mitigations can be put in place. A faulty system that presents an inaccurate operating picture can unknowingly put agents at risk. Potential failures can be averted through health monitoring, thereby increasing system availability. The ability to isolate faults and failures to the LRU level can also reduce system down time.

4.5 SUPPORTABILITY AND SUSTAINMENT (INTEGRATED LOGISTICS SUPPORT)

IFT ORD 58 System support shall provide 24/7 on-call technical assistance.

Rationale: USBP conducts operations 24/7 and needs the ability to discuss system issues/questions, reset passwords, etc. with a "helpdesk" that is available 24/7.

IFT ORD 59 System support shall provide the means to assess system performance against KPPs over the life of the system.

Rationale: Operation and maintenance over time can degrade system performance; the extent of this performance degradation must be documented in order to assess the impact on the mission and plan operational mitigations accordingly.

4.6 SURVIVABILITY

IFT ORD 60 The system shall be protected against unauthorized access to the system and its data in accordance with DHS/CBP policies and procedures.

Rationale: The system must be secured in a manner that prevents unauthorized persons from tampering with or disabling the system through physical and other means. (b) (7)(E)

IFT ORD 61 The system shall be hardened against vandalism.

Rationale: Border threats frequently attempt to disable/degrade systems through any available means, to include (b) (7)(E)

4.7 HUMAN FACTORS/HUMAN MACHINE INTERFACE

IFT ORD 62 The system shall (b) (7)(E) .

Rationale: (b) (7)(E)

IFT ORD 63 The system shall accommodate operators ranging from (b) (7)(E), viewing displays and controls, ingress/egress and personnel equipment and facilities.

Rationale: The system must physically accommodate the majority of operators and minimize the potential for fatigue or injury over the course of short and long term use.

4.8 SAFETY

IFT ORD 64 The system shall be safe to operate and maintain as required by applicable Occupational Safety and Health Administration (OSHA) standards and CBP policies and procedures.

Rationale: As stated.

4.9 ENVIRONMENTAL CONSIDERATIONS

IFT ORD 65 The system shall (b) (7)(E)

Rationale: (b) (7)(E)

IFT ORD 66 The system shall (b) (7)(E)

[11] (b) (7)(E)

Rationale: (b) (7)(E)

IFT ORD 67 The system shall (b) (7)(E)

Rationale: (b) (7)(E)

4.10 TRAINING REQUIREMENTS

IFT ORD 68 System operation shall not require skill sets beyond those currently required for USBP agents and Sector Enforcement Specialists.

Rationale: USBP must be able to use existing work force to operate the system and currently had no plans to create a new occupational specialty for this position; a need to recruit and hire individuals with a different skill set can have substantial personnel implementation and cost impacts.

IFT ORD 69 System training material shall be an integrated part of the system support package.

Rationale: As stated.

IFT ORD 70 The system shall provide (b) (7)(E)

Rationale: (b) (7)(E)

5 KEY PERFORMANCE PARAMETERS

Table 2. Key Performance Parameters

Parameter	Threshold	Objective
(b) (7)(E)		

6 GLOSSARY

Table 3. Glossary of Terms

TERM	DEFINITION
Area of Interest	A targeted area within a USBP Station's AoR that requires surveillance due to the risk level associated with border threat exploitation.
Area of Coverage	The resulting area, considering installation location of all units, (b) (7)(E) [redacted] etc., within which USBP can successfully conduct surveillance activities using the system or a combination of systems.
Automated	Conducted by the system rather than the operator.
Availability	The ratio of the system's mission capable time (MCT) divided by total time, which is the sum of mission capable time plus down time. Mathematically, this can be described by the following equation: $Ao = \frac{\sum MCT_{COP}}{\sum MCT_{COP} + \sum Down\ Time_{COP}} \times \frac{\sum MCT_{IFT\ units}}{\sum MCT_{IFT\ units} + \sum Down\ Time_{IFT\ units}}$
Classify	To determine the level of threat or intent of the detected entity.
Detect	To discover possible illegal traffic.
Deter	To dissuade illegal cross border activity into and out of the United States by creating and conveying a certainty of immediate interdiction upon entry.
Identify	To determine what the detected entity is (human, animal, conveyance, unknown).
IFT System	The entirety of all IFT subsystems, to include the COP, operator workstations, all associated processing equipment, all deployed IFT units, and any supporting power and communications subsystems.
IFT Unit	The deployed surveillance equipment that includes the (b) (7)(E) [redacted]
Persistent Surveillance	The ability to continuously detect, track, identify and classify 24 hours a day, seven days a week.
Predict	To anticipate illegal traffic actions prior to illegal activity.
Real Time	A (b) (7)(E) [redacted] to facilitate effective employment of the system.
Respond	To employ the appropriate level of law enforcement resources to successfully address illegal traffic.
Resolve	To take final CBP action, whether criminally, administratively, or other, against apprehended illegal traffic. [This includes capture data, process information, etc. This may also include the release of legitimate traffic with no law enforcement action.]
Surveillance Area	The area within which a single system is capable of detecting, tracking, identifying and classifying illegal incursions. The surveillance area does not consider (b) (7)(E) [redacted].
Track	To follow the progress/movements of possible illegal traffic.

7 ACRONYMS

Ao	Operational Availability
AoA	Analysis of Alternatives
AoC	Area of Coverage
AoI	Area of Interest
AoR	Area of Responsibility
ATV	All Terrain Vehicle
BP	Border Patrol
BPA	Border Patrol Agent
C2	Command and Control
C4I	Command, Control, Communication, Coordination and Intelligence
CBP	Customs and Border Protection
COI	Critical Operational Issue
COP	Common Operational Picture
COTS	Commercial Off-the-Shelf
DHS	Department of Homeland Security
DOI	Department of Interior
FCC	Federal Communications Commission
FOC	Full Operational Capability
FOV	Field of View
GOTS	Government Off-the-Shelf
GPS	Global Positioning System
ICAD	Intelligent Computer Assisted Detection
IFT	Integrated Fixed Towers
IOC	Initial Operational Capability
IoI	Item of Interest
IR	Infrared
KPP	Key Performance Parameter
LMR	Land Mobile Radio
LoS	Line of Sight

LRU	Line Replacement Unit
MCT	Mission Capable Time
MDT	Mean Down Time
MFR	Memorandum for Record
MLDT	Mean Logistics Down Time
MNS	Mission Needs Statement
MPH	Miles Per Hour
MSC	Mobile Surveillance Capability
[redacted]	(b) (7)(E)
MTBCF	Mean Time Between Critical Failure
MTTR	Mean Time To Repair
MVSS	Mobile Video Surveillance System
NDI	Non-Developmental Items
NEPA	National Environmental Policy Act
NTIA	National Telecommunication and Information Administration
NVG	Night Vision Goggles
O	Objective
O&M	Operations & Maintenance
OJT	On the Job Training
OIT	Office of Information and Technology
OTD	Office of Training and Development
PIR	Post Implementation Review
PA	Patrol Agent
[redacted]	(b) (7)(E)
SBI	Secure Border Initiative
T	Threshold
T3	Train the Trainer
TBD	To Be Determined
UAS	Unmanned Aircraft System
UGS	Unattended Ground Sensors

U.S.	United States
USBP	United States Border Patrol

APPENDIX 1: REFERENCES

The government documents listed in Table 4 support the IFT program acquisition and were referenced in the Operational Requirements Document.

Table 4. Government Documents

Document Number	Document Title	Date
N/A	Arizona Border Surveillance Technology Deployment Plan – Briefing to the Secretary of DHS	July 2010
OTIA05-AZBSTP-00-000001	Arizona Border Surveillance Technology Plan Concept of Operations Document, Draft V0.03	June 22, 2011
N/A	CBP Concept of Operations (SBInet Enabled), Version 2.0	June 26, 2008
N/A	SBInet Mission Needs Statement (MNS), Version 1.0	October 1, 2006
N/A	SBInet Operational Requirements Document, Version 1.0	March 6, 2007
N/A	Secure Border Initiative SBI) Design Reference Mission (DRM) – Great Lakes and Southwest Border, Office of Border Patrol Sectors, Version 1.0	May 2010
N/A	U.S. Customs and Border Protection Fiscal Year 2009-2014 Strategic Plan	July 2009
N/A	CBP's Missions, Goals, and Priorities, FY2011-2013	March 24, 2011
N/A	Operational Test Agency Evaluation Report for the Secure Border Initiative Network (SBInet) Block 1.0	March 2011
102-01	Acquisition Management Directive	January 20, 2010

APPENDIX 2: REQUIREMENTS TRACEABILITY MATRIX

Table 5 shows the traceability between the operational requirements, COIs, the applicable capability. To facilitate cost-effectiveness and schedule tradeoffs, the requirements have also been prioritized as follows:

- Priority 1 (KPP): Deviation below the threshold requires approval in accordance with DHS Acquisition Management Directive 102-01
- Priority 2: Deviation below the threshold requires USBP endorsement
- Priority 3: Deviation below the threshold requires USBP notification

Once the tradeoff analysis is complete and the IOC/FOC capability has been finalized, the Program Manager, through the Component Acquisition Executive, will submit a formal Memorandum for Record (MFR) to USBP. The MFR will request the endorsement of and/or provide notification of the operational requirement deviation(s) for the acquisition.

Table 5. Operational Requirements Summary

Rqmnt ID	Operational Requirement	Mission Element	COI	Capa-bility	Pri-ority
IFT ORD 01	(b) (7)(E)	(b) (7)(E)			
IFT ORD 02					
IFT ORD 03					
IFT ORD 04					
IFT ORD 05					
IFT ORD 06					
IFT ORD 07					

Rqmnt ID	Operational Requirement	Mission Element	COI	Capa-bility	Pri-ority
IFT ORD 08	(b) (7)(E)	(b) (7)(E)			
IFT ORD 09					
IFT ORD 10					
IFT ORD 11					
IFT ORD 12					
IFT ORD 71					
IFT ORD 13					
IFT ORD 14					
IFT ORD 15					
IFT ORD 16					
IFT ORD 72					

Rqmnt ID	Operational Requirement	Mission Element	COI	Capa-bility	Pri-ority
IFT ORD 17	(b) (7)(E)	(b) (7)(E)			
IFT ORD 18					
IFT ORD 19					
IFT ORD 20					
IFT ORD 21					
IFT ORD 22					
IFT ORD 23					
IFT ORD 24					
IFT ORD 25					
IFT ORD 26					
IFT ORD 27					
IFT ORD 28					

Rqmnt ID	Operational Requirement	Mission Element	COI	Capa-bility	Pri-ority
IFT ORD 29	(b) (7)(E)	(b) (7)(E)			
IFT ORD 30					
IFT ORD 31					
IFT ORD 32					
IFT ORD 33	The system shall geospatially display the international boundary line.				
IFT ORD 34	(b) (7)(E)				
IFT ORD 35					
IFT ORD 036					
IFT ORD 37					
IFT ORD 38					
IFT ORD 39					
IFT ORD 40					

Rqmnt ID	Operational Requirement	Mission Element	COI	Capa-bility	Pri-ority
IFT ORD 41	(b) (7)(E)	(b) (7)(E)			
IFT ORD 42					
IFT ORD 43					
IFT ORD 44					
IFT ORD 45					
IFT ORD 46	The system shall be capable of utilizing existing CBP communications infrastructure when such infrastructure is available.				
IFT ORD 47	(b) (7)(E)				
IFT ORD 48					
IFT ORD 49	The system shall not interfere with or degrade the operation of other CBP equipment.				
IFT ORD 50	The system shall be approved for secure operations in accordance with applicable CBP and DHS security policies and procedures.				
IFT ORD 51	(b) (7)(E)				
IFT ORD 52					
IFT ORD 54					
IFT ORD 55	**The system operational availability (Ao) shall be equal to or greater than** (b) (7)(E) **where Ao is defined as mission capable time (sum of all mission critical subsystems and units) divided by total time (mission capable time plus down time). (KPP)**				
IFT ORD 56	The system MDT shall be (b) (7)(E)				

Rqmnt ID	Operational Requirement	Mission Element	COI	Capa-bility	Pri-ority
IFT ORD 57	The system shall report mission critical failures to the operator (T) / and provide system health status when prompted by the operator (O).	(b) (7)(E)			
IFT ORD 58	System support shall provide 24/7 on-call technical assistance.				
IFT ORD 59	System support shall provide the means to assess system performance against KPPs over the life of the system.				
IFT ORD 60	The system shall be protected against unauthorized access to the system and its data in accordance with DHS/CBP policies and procedures.				
IFT ORD 61	The system shall be hardened against vandalism.				
IFT ORD 62	(b) (7)(E)				
IFT ORD 63	The system shall accommodate operators ranging from [redacted] viewing displays and controls, ingress/egress and personnel equipment and facilities.				
IFT ORD 64	The system shall be safe to operate and maintain as required by applicable OSHA standards and CBP policies and procedures.				
IFT ORD 65	(b) (7)(E)				
IFT ORD 66					
IFT ORD 67					
IFT ORD 68	System operation shall not require skill sets beyond those currently required for USBP agents and Sector Enforcement Specialists.				
IFT ORD 69	System training material shall be an integrated part of the system support package.				
IFT ORD 70	(b) (7)(E)				